INSI

Syllabus de la Formation Cyber Attaque et Administration Réseaux et Systèmes

Aucune description

Niveau : Avancée

Prix : à partir de 0,00 Ar HT

Durée : jours | heures

Place : personnes

Sessions

Objectifs de cette formation

- Comprendre les bases des cyberattaques et les méthodes de sécurisation des réseaux et systèmes.
- Appliquer les meilleures pratiques pour sécuriser les infrastructures réseau et système.
- Identifier et répondre efficacement aux incidents de sécurité.
- Utiliser des outils de pentesting pour évaluer la sécurité des systèmes.
- Développer des stratégies de défense pour protéger les actifs informatiques de l’entreprise.

Programmes de cette formation

- - Introduction aux Cyberattaques et Sécurité Réseau Matinée
    - Objectifs de la formation
    - Tour de table des participants
    - Historique des cyberattaques célèbres
    - Typologie des cyberattaques (phishing, malware, ransomware, DDoS, etc.)
    - Principes de base de la cybersécurité (confidentialité, intégrité, disponibilité)
    - Modèle CIA (Confidentiality, Integrity, Availability)
    - Modèle OSI et TCP/IP
    - Configuration de base des routeurs et des commutateurs
    - Protocoles de routage (RIP, OSPF, BGP)
    - Pare-feu et systèmes de détection d’intrusion (IDS/IPS)
    - VPN et réseaux privés virtuels
    - Segmentation réseau et VLAN
- - Administration des Systèmes et Sécurité Matinée
    - Introduction aux systèmes d’exploitation (Windows, Linux)
    - Gestion des utilisateurs et des permissions
    - Surveillance et gestion des ressources système
    - Mise à jour et gestion des correctifs
    - Antivirus et antimalware
    - Configuration sécurisée des systèmes
    - Hardening des systèmes (Linux, Windows)

- Configuration sécurisée des serveurs web (Apache, Nginx)
- Sécurisation des bases de données (MySQL, PostgreSQL)
- Identification et analyse des incidents
- Réponse aux incidents et plan de reprise
- Analyse post-incident et amélioration continue

- - Pratiques Avancées et Études
    - Exploitation des vulnérabilités (buffer overflow, injection SQL)
    - Attaques sur les réseaux sans fil (Wi-Fi hacking)
    - Ingénierie sociale et manipulation psychologique
    - Utilisation des outils de scan de vulnérabilités (Nessus, OpenVAS)
    - Introduction au pentesting (Metasploit, Kali Linux)
    - Analyse de cyberattaques réelles
    - Discussion des leçons apprises et des stratégies de défense
    - Mise en place d’un environnement de test
    - Exécution et analyse d’une cyberattaque simulée
    - Développement de stratégies de mitigation